

BGK:AL: F#2023V01592

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA,

Plaintiff,

v.

ANY AND ALL VIRTUAL CURRENCY  
ON DEPOSIT IN BINANCE ACCOUNT  
ASSOCIATED WITH USER ID 16130005  
AND EMAIL ADDRESS  
LCD.JASON@GMAIL.COM HELD IN  
THE NAME OF HARISH KUMAR, UP  
TO AND INCLUDING THE SUM OF  
1,507,314.00 DOGECOIN (DOGE),  
171,057,133.00 SHIBA INU COIN (SHIB),  
1,621,915.00 BITTORRENT (BTTC),  
3,925.75 RIPPLE (XRP),  
114,489.00 DENT TOKEN (DENT),  
24,257.00 FUNTOKEN (FUN),  
58,441.00 VETHOR TOKEN (VTHO),  
11,916.00 TOKENCLUB (TCT),  
4,914,845.00 APENFT (APENFT),  
AND ALL PROCEEDS TRACEABLE  
THERETO;

ANY AND ALL VIRTUAL CURRENCY ON  
DEPOSIT IN BINANCE ACCOUNT  
ASSOCIATED WITH USER ID 132479102  
AND EMAIL ADDRESS  
RAJKUMARI957962@GMAIL.COM HELD IN  
THE NAME OF RAJ KUMARI, UP TO AND  
INCLUDING THE SUM OF  
3,689.554732000 TERRA TOKEN (LUNA),  
0.007581900 CARDANO COIN (ADA),  
0.067382060 VECHAIN TOKEN (VET),  
0.042600000 DOGECOIN (DOGE),  
0.000018710 BINANCE COIN (BNB),  
93,019.58848700 POLYGON (MATIC),  
205,113,352.5000 SHIBA INU COIN (SHIB),

**VERIFIED COMPLAINT  
IN REM**

Civil Action No:

24-CV-8514

(\_\_\_\_\_, J.)

(\_\_\_\_\_, M.J.)

58.171340110 ETHEREUM CLASSIC (ETC),  
100.000000790 TETHER (USDT),  
0.002690000 RIPPLE (XRP),  
0.010824270 ETHEREUM (ETH),  
0.033895900 STELLAR (XLM),  
984.8960000 VETHOR TOKEN (VTHO),  
0.008990000 INTERNET COMPUTER  
PROTOCOL TOKEN (ICP),  
AND ALL PROCEEDS TRACEABLE  
THERETO; and

ANY AND ALL VIRTUAL CURRENCY ON  
DEPOSIT IN BINANCE ACCOUNT  
ASSOCIATED WITH USER ID 104645579  
AND EMAIL ADDRESS  
IN9313330339\_MOBILEUSER@BINANCE.COM  
HELD IN THE NAME OF RAKESH KUMAR  
ATHOTRA, UP TO AND INCLUDING THE  
SUM OF  
71,051.485100 CARDANO COIN (ADA),  
334.085580 SOLANA COIN (SOL),  
23,709,938.900 ECASH (XEC) ,  
56.35100 GALA TOKEN (GALA) ,  
0.002916800 SANTOS FC FAN TOKEN  
(SANTOS),  
0.056190110 HIGHCOIN (HIGHT),  
27,867,735.4700 SHIBA INU COIN (SHIB),  
0.64600 AUTOMATA TOKEN (ATA),  
0.000000260 BITCOIN (BTC),  
0.000018020 ETHEREUM (ETH),  
0.000329810 LITECOIN (LTC),  
0.686685480 TETHER (USDT),  
0.005774580 CHAINLINK (LINK),  
0.000493810 ETHEREUM CLASSIC (ETC),  
0.003250000 RIPPLE (XRP),  
0.002145210 UNISWAP TOKEN (UNI),  
0.018600000 POLYGON (MATIC),  
0.000014860 BINANCE/PAXOS USD (BUSD),  
359.6600000 STELLAR (XLM),  
AND ALL PROCEEDS TRACEABLE  
THERETO.

Defendants *in rem*,

-----X

Plaintiff, the United States of America, by its attorney, BREON PEACE, United States Attorney for the Eastern District of New York and Artemis Lekakis, Assistant United States Attorney, of counsel, for its complaint herein, alleges upon information and belief as follows:

### **NATURE OF THE ACTION**

1. The United States of America brings this civil action *in rem* to forfeit and condemn to the exclusive use and benefit of the United States the above-captioned Defendants *in rem*, and all proceeds traceable thereto, pursuant to Title 18, United States Code, Section 981(a)(1)(C) as property which constitutes or is derived from proceeds of offenses constituting a “specified unlawful activity,” to wit, wire fraud, in violation of Title 18, United States Code, Section 1343.

### **JURISDICTION AND VENUE**

2. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

3. Venue lies in the Eastern District of New York pursuant to 28 U.S.C. §§ 1355 and 1395.

### **THE DEFENDANTS *IN REM***

4. The Defendants *in rem* consist of:
- (a) any and all virtual currency on deposit in the Binance Account associated with User ID 16130005 (“Account 005”) and email address lcd.jason@gmail.com held in the name of Harish Kumar, up to and including the sum of 1,507,314.00 Dogecoin (DOGE), 171,057,133.00 Shiba Inu Coin (SHIB), 1,621,915.00 BitTorrent (BTTC), 3,925.75 Ripple (XRP), 114,489.00 Dent Token (DENT), 24,257.00 Funtoken (FUN), 58,441.00 Vethor Token (VTHO), 11,916.00 TokenClub (TCT),

4,914,845.00 ApeNFT (APENFT), and all proceeds traceable thereto (hereinafter, “Account 005”);

(b) any and all virtual currency on deposit in Binance account associated with User Id 132479102 (“Account 102”) and email address rajkumari957962@gmail.com held in the name of Raj Kumari, up to and including the sum of 3,689.554732000 Terra Token (LUNA), 0.007581900 Cardano Coin (ADA), 0.067382060 Vechain Token (VET), 0.042600000 Dogecoin (DOGE), 0.000018710 Binance Coin (BNB), 93,019.58848700 Polygon (MATIC), 205,113,352.5000 Shiba Inu Coin (SHIB), 58.171340110 Ethereum Classic (ETC), 100.000000790 Tether (USDT), 0.002690000 Ripple (XRP), 0.010824270 Ethereum (ETH), 0.033895900 Stellar (XLM), 984.8960000 Vethor Token (VTHO), 0.008990000 Internet Computer Protocol Token (ICP), and all proceeds traceable thereto (hereinafter, “Account 102”); and

(c) any and all virtual currency on deposit in Binance account associated with User ID 104645579 (“Account 579”) and email address in9313330339\_mobileuser@binance.com held in the name of Rakesh Kumar Athotra, up to and including the sum of 71,051.485100 Cardano Coin (ADA), 334.085580 Solana Coin (SOL), 23,709,938.900 ECash (XEC), 56.35100 Gala Token (GALA), 0.002916800 Santos FC Fan Token (SANTOS), 0.056190110 Highcoin (HIGHT), 27,867,735.4700 Shiba Inu Coin (SHIB), 0.64600 Automata Token (ATA), 0.000000260 Bitcoin (BTC), 0.000018020 Ethereum (ETH), 0.000329810 Litecoin (LTC), 0.686685480 Tether (USDT), 0.005774580 Chainlink (LINK), 0.000493810 Ethereum Classic (ETC), 0.003250000 Ripple (XRP), 0.002145210 Uniswap Token (UNI), 0.018600000 Polygon (MATIC), 0.000014860 Binance/Paxos Usd (BUSD), 359.6600000 Stellar (XLM), and all proceeds traceable thereto (hereinafter, “Account 579”)

(hereinafter, collectively Account 005, Account 102 and Account 579 shall be referenced as the “SUBJECT ACCOUNTS”).

5. According to information that law enforcement agents obtained from Binance Exchange, Account 005 is associated with Binance Exchange User ID 16130005 and held in the name of Harish Kumar who resides in India. The email associated with this account is lcd.jason@gmail.com and Account 005 was established on or about December 23, 2017.

6. The law enforcement investigation of the Binance Exchange also developed information establishing that Account 102 is associated with Binance Exchange

User ID 132479102 and held in the name of Raj Kumari who resides in India. The email associated with this account is rajkumari957962@gmail.com. Account 102 was created on or about April 23, 2021.

7. Further law enforcement investigations based on information from Binance Exchange determined that Account 579 is associated with Binance Exchange User ID 104645579 and held in the name of Rakesh Kumar Athotra, who resides in India. The email associated with this account is in9313330339\_mobileuser@binance.com. Account 579 was created on or about March 25, 2021.

### **STATUTORY AND REGULATORY FRAMEWORK**

8. Under Title 18, United States Code, Section 1343, it is unlawful to devise any scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, by transmitting or causing to be transmitted by means of wire in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

9. Under 18 U.S.C. § 981(a)(1)(C), “[t]he following shall be subject to forfeiture to the United States: . . . (C) Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of . . . any offense constituting ‘specified unlawful activity’ (as defined in section 1956(c)(7) of this title).”

10. Pursuant to Title 18, United States Code, Section 1961(1)(B), as incorporated by Title 18, United States Code, Section 1956(c)(7)(A), the term “specified unlawful activity” includes violations of Title 18, United States Code, Section 1343.

### **THE INVESTIGATION**

11. In or about April 2021, law enforcement became aware of a fraud scheme that targeted certain owners of cryptocurrency (the “Victims”), specifically individuals who had an account with the cryptocurrency exchange Coinbase.

12. The scheme operated by emailing the Victims, one of whom resides in the Eastern District of New York, and falsely advising them that there were issues with their Coinbase accounts, when in reality there was no issue with any of the Victims’ Coinbase accounts.

13. Thereafter, the Victims either clicked on a link in a fake e-mail that led them to, or they otherwise found, a purported Coinbase telephone number and called the “Coinbase” customer service telephone number listed on that page.

14. However, Coinbase does not offer telephone-based customer service or provide any phone number on the internet for Coinbase customers to call. As a result, the false “Coinbase” customer service phone number (“False Coinbase Service Number”) posted on the internet did not connect with any phones at Coinbase, but instead connected to phone(s) that the fraud scheme perpetrators operated.

15. Once the Victims called this False Coinbase Service Number and started speaking with the fraud scheme perpetrators over the phone, the fraud scheme perpetrators impersonated Coinbase customer support representatives and directed the Victims to provide information (such as account numbers and/or passwords) and/or take actions (such as giving remote control of their laptop to the “customer service representatives”).

16. The information obtained and/or actions conducted under false pretenses allowed the fraud scheme perpetrators to transfer or cause the Victims to transfer some or all

of their Coinbase cryptocurrency holdings initially to cryptocurrency mid-point wallets either owned or controlled by the fraud scheme perpetrators and thereafter to the Subject Accounts.

17. To date, the investigation has identified at least four individuals who were Victims of this scheme.

**Victim-1**

18. On or about April 14, 2021, law enforcement learned that Victim-1, an individual who had purchased certain cryptocurrency in the form of *inter alia* Bitcoin, Ethereum and XLM over the last four to five years and had his<sup>1</sup> investments in these cryptocurrencies experience significant growth, had been defrauded of nearly \$1.5 million in cryptocurrency that he held in the account that he maintained at the Coinbase cryptocurrency exchange.

19. Victim-1 informed law enforcement that on or about April 5, 2021, he received an e-mail from what appeared to be a Coinbase email account indicating that there was a problem with the bank payments that he had been using to fund purchases of cryptocurrency in his account.

20. In response to this email, Victim-1 either clicked on a link in the e-mail, or otherwise contacted Coinbase to ensure that his accounts were secure. Ultimately, Victim-1 arrived at a screen that displayed a purported telephone number for Coinbase customer service, which was 888-312-3871.

---

<sup>1</sup> To avoid inadvertently providing any identifying information relating to any of the Victims (including, but not limited to gender identification), “he,” “his” and/or “him” shall be used in conjunction with all Victim-related references.

21. Upon dialing this number, Victim-1 spoke with an individual identifying himself as “Calvin,” whom Victim-1 described as speaking with an “Indian” accent and as sounding younger. Calvin told Victim-1 that he worked for Coinbase and that he could help Victim-1 secure his accounts.

22. At some point during the conversation, Calvin asked Victim-1 for information related to Victim-1’s Coinbase account, which Victim-1 provided. Thereafter, Calvin instructed Victim-1 to change the “authenticator” and “security code” for his Coinbase account. In addition, Calvin, still posing as a Coinbase employee, told Victim-1 that he needed to remotely connect and gain access to Victim-1’s computer. At some point, to enable this remote access, Calvin sent Victim-1 an e-mail that had a red button, and instructed Victim-1 to click on that button. Victim-1 complied.

23. After clicking the red button, Victim-1’s computer screen turned blue for approximately 15 minutes and displayed a message that stated, “Wait one moment.” Calvin told Victim-1 that it would take approximately two (2) days for the issue relating to the payments from his bank account to be resolved and for the Coinbase account to be secured.

24. By April 14, 2021, Victim-1 realized that Calvin was not a Coinbase employee, and, apparently as a result of his interactions with Calvin, Victim-1 was locked out of his Coinbase account.

25. On April 26, 2021, Victim-1 regained access to his Coinbase Account, but only on a read-only access. After regaining access to his Coinbase Account, Victim-1 discovered that the cryptocurrency previously contained in his account, valued at approximately \$1.5 million in the form of Bitcoin and Ethereum, had been transferred out of Victim-1’s Coinbase



account on or around April 7, 2021 without Victim-1's knowledge, authorization or permission.

26. Records show that *inter alia* approximately 478 Ethereum were transferred out of Victim-1's Coinbase account, into multiple mid-point cryptocurrency wallets in multiple-stage transactions. Blockchain tracing analysis revealed that one or more of these mid-point wallets that were used for the fraudulent and/or unauthorized transfers of Victim 1's cryptocurrency also were used in the fraudulent and/or unauthorized transfers of the other Victims' cryptocurrency.

27. Further, cryptocurrency tracing analysis established that through these fraudulent and/or unauthorized transactions, approximately 238.99 Ethereum of Victim 1's cryptocurrency ultimately was transferred to Account 005 and approximately 253.95 Ethereum of Victim 1's cryptocurrency ultimately was transferred to Account 102.

### **Victim-2**

28. On or about, May 13, 2021, law enforcement learned that Victim-2, a resident of Brooklyn, New York, also was defrauded by the same scheme. Victim-2 informed law enforcement that on or about May 9, 2021, he took action to connect his Coinbase account to his Binance account to facilitate fund transfers between the two accounts.

29. Later that day, Victim-2, was using his laptop within the geographic boundaries of the Eastern District of New York. In the course of using his laptop, he searched and navigated to what appeared to be a Coinbase website. On this website, Victim-2 submitted a help ticket to assist with the fund transfers. Victim-2 thereafter received a phone call from an unknown male ("UM1") whom Victim-2 believed to be associated with Coinbase.

30. In the course of purporting to provide “Coinbase” assistance to Victim-2, the UM1 sent Victim-2 an email with a link and requested that Victim-2 click the link to allow remote access to Victim-2’s computer to assist with the fund transfer issue.

31. Victim-2 informed law enforcement that initially, Victim-2 clicked the link and gave permission to the UM1 to access the laptop remotely.

32. Thereafter, Victim-2 noticed that through the remote access that he had just given to the UM1, the UM1 was attempting to access Victim-2’s files that he did not authorize the UM1 to access. Specifically, Victim-2 noticed that the UM1 was trying to access files and folders on his Windows computer.

33. Immediately at that point, Victim-2 cancelled the remote access that had been given to the UM1 and deleted the previously downloaded application that the UM1 had used to gain that remote access.

34. After this incident, Victim-2 was unable to access his Coinbase account and was unable to reach Coinbase customer service.

35. Records show that, following the May 9, 2021 telephone call with the UMI, approximately 1.2 Ethereum were transferred out of Victim-2’s into multiple mid-point cryptocurrency wallets in multiple-stage transactions. Blockchain tracing analysis revealed that one or more of these mid-point wallets that were used for the fraudulent and/or unauthorized transfers of Victim 2’s cryptocurrency also were used in the fraudulent and/or unauthorized transfers of the Victim 1’s cryptocurrency.

36. Law enforcement blockchain and cryptocurrency tracing analysis established that through these fraudulent and/or unauthorized transactions, approximately 1.2 Ethereum of Victim 2’s cryptocurrency ultimately was transferred to Account 579.

**Victim-3**

37. In the course of the investigation, law enforcement officers determined that the same fraud scheme that caused Victim-1 and Victim-2 to lose funds also caused unauthorized, illicit and/or fraudulent transfers of cryptocurrency from Victim-3's Coinbase account and caused that cryptocurrency to be deposited into one or more of the Subject Accounts.

38. Analysis of transactions occurring on Coinbase during this period indicated that fraudulent, unauthorized and/or illicit transfers were occurring over multiple user accounts, including, but not limited to, those involving the Victims here, during the relevant period.

39. All of these transfers are part of the same scheme as that involving the other Victims identified herein, based on *inter alia* the fact that these fraudulent, unauthorized and/or illicit transactions also involved one or more of the mid-point cryptocurrency wallets and/or one or more of the Subject Accounts

40. Specifically, the information developed through this analysis revealed that on or about May 7, 2021, which was during roughly the same time frame that unauthorized and illicit transfers of cryptocurrency were occurring with respect to the accounts of the other Victims, unauthorized and illicit transfers occurred with respect to cryptocurrency held in the Coinbase account of Victim-3.

41. Law enforcement investigations determined that during this period of time, Victim-3's account had been compromised and someone logged into his account, without his authorization and changed the two-factor code used when logging into his account, and ostensibly also changed the e-mail address associated with Victim-3's Coinbase account.

Thereafter Victim-3 no longer received the two-factor codes and Victim-3 no longer received e-mails that Coinbase was sending about his account.

42. Subsequent to these unauthorized permission and e-mail changes to Victim-3's account, there were unauthorized, fraudulent and/or illicit transfers of cryptocurrency out of Victim-3's Coinbase account, which totaled approximately 6.4 Ethereum. These fraudulent, unauthorized and illicit cryptocurrency transfers were performed in multiple stages and involved one or more of the same mid-point cryptocurrency wallets that were used in fraudulent transfers of the other Victims' cryptocurrency.

43. Law enforcement review of Coinbase e-mail records established that Victim-3 never authorized nor intended for the transfer of Ethereum cryptocurrency out of his Coinbase Account.

44. Law enforcement blockchain and cryptocurrency tracing analysis determined that the unauthorized, fraudulent and illicit cryptocurrency transfers of approximately 6.4 Ethereum out of Victim-3's Coinbase account ultimately resulted in the transfer of Victim-3's cryptocurrency into Account 579.

#### **Victim-4**

45. On or about May 3, 2021, Victim-4 wanted to increase the trading limits for his Coinbase account. To achieve this, Victim-4 Googled a customer service number for Coinbase, found a telephone number for purported Coinbase customer service and called the telephone number that he found on Google.

46. When the call went through, Victim-4 spoke with an individual who identified himself as "Calvin." During the phone call, Calvin and Victim-4 discussed Victim-4's interest in increasing the dollar limits for trading on his account. In addition, during the conversation,

Calvin brought up to Victim-4 the concept of a “more secure” cryptocurrency wallet called the “purse.”

47. At Calvin’s suggestion, Victim-4 agreed to try the increased security of the “purse” for his Coinbase cryptocurrency account. Victim-4 informed law enforcement that Calvin agreed to take the necessary action to transfer Victim-4’s account to the “purse,” and Victim-4 remembered Calvin telling them that the transfer would be completed within approximately 48 hours.

48. Thereafter, on or about May 5, 2021, Victim-4 noticed that approximately \$49,600 held in variations comprised of Bitcoin, Litecoin, Ethereum and Uniswap cryptocurrency had been transferred out of his Coinbase account.

49. Victim-4 did not authorize any transfer of this cryptocurrency out of his Coinbase account.

50. Further, after this incident, Victim-4 was unable to access his Coinbase account, and was unable to reach Coinbase customer service at the number retrieved from his internet search.

51. Several days after this incident, Victim 4 tried again to Google a telephone number for Coinbase customer service, but unlike the prior time, on that occasion, there was no telephone number that appeared for Coinbase customer service.

52. Approximately six days after the cryptocurrency transfer at issue, Victim-4 received a call from the same number at which he had previously reached “Calvin.” When Victim-4 answered, Calvin immediately hung up.

53. During the course of the investigation, law enforcement agents determined that that approximately 3.8 Ethereum, .508 Bitcoin, 11.33 Litecoin and 115.139 Uniswap were transferred out of Victim-4's Coinbase account.

54. Cryptocurrency tracing analysis revealed that Victim-4's cryptocurrency was transferred out of his Coinbase account using one or more of the same cryptocurrency wallets that were involved in the unauthorized and illicit withdrawals from one or more of the other Victims.

55. Blockchain ledger tracing analysis established that approximately 3.8 of Victim-4's Ethereum ultimately was transferred from one or more of the mid-point wallets used to defraud on or more of the other Victims into Account 102. Similarly, using the same common mid-point wallet(s), approximately .508 of Victim-4's Bitcoin was transferred into Account 579.

**THE SUBJECT ACCOUNTS  
AND SUBSEQUENT DEVELOPMENTS**

56. The cryptocurrency tracing analyses conducted in the course of the law enforcement investigation established that after withdrawal from the Coinbase accounts of all of the Victims, the cryptocurrency from these different victims was transferred into many of the same midpoint and ultimately endpoint cryptocurrency wallets, which further supports a determination that the fraud was part of a related and/or coordinated effort by the owners of the Subject Accounts identified above.

57. The Victims' cryptocurrency had been illicitly and without authorization transferred out of their Coinbase accounts and into one or more of the Subject Accounts, and then the Victims' cryptocurrency was exchanged for other cryptocurrencies, including, but not

limited to BitTorrent, Binance Token, APENFT, Dent, Dogecoin, Fun Token, Polygon, Ripple, Shiba Inu, TetherUS, Tokenclub Token, Vethor Token, Cardano, Internet Computer, Ethereum, Ethereum Classic, Stellar Lumens, Terra, VeChain and VeThor Token.

58. Based on the law enforcement tracing analysis, on March 16, 2022, the Honorable James R. Cho, United States Magistrate, Eastern District of New York, issued seizure warrants for the seizure of the defendants in rem in the Subject Accounts finding probable cause that the Subject Accounts contained the proceeds of wire fraud, in violation of 18 U.S.C. §1343.

59. Subsequent to that seizure warrant the United States transferred the Victims' cryptocurrency that could be recovered, into one or more cryptocurrency wallets under the possession, custody and control of the United States government's Federal Bureau of Investigation.

60. Upon information and belief, the government of the federal republic of India currently is investigating one or more of the owners of the Subject Account and pursuing action against one or more of the owners of the Subject Accounts based on *inter alia* one or more of the fraudulent actions alleged above.

#### **CLAIM FOR RELIEF**

61. Plaintiff repeats and realleges the allegations contained in paragraphs 1 through 60 as if set forth fully herein.

62. The Subject Accounts represent proceeds traceable to a violation of an offense constituting a specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), to wit, 18 U.S.C. § 1343, wire fraud.


63. As a result, the Subject Accounts and all proceeds traceable thereto are liable to condemnation and forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C).

WHEREFORE, Plaintiff, United States of America, requests that a warrant of this Court be issued for the arrest of the Subject Accounts; that notice of these proceedings be given to all interested persons; that the Subject Accounts be forfeited and condemned to the use of the United States of America; that the Plaintiff be awarded its costs and disbursements in this action and for such other and further relief as this Court deems just and proper.

Dated: Brooklyn, New York  
December 12, 2024

BREON PEACE  
UNITED STATES ATTORNEY

By: \_\_\_\_\_

  
Artemis Lekakis  
Assistant United States Attorney  
271 Cadman Plaza East  
Brooklyn, New York 11201  
(718) 254-6096

*Attorney for Plaintiff*




VERIFICATION

JOHN REUTHER hereby declares as follows:

1. I am a Task Force Officer with the Federal Bureau of Investigation, duly appointed according to law and acting as such.
2. I have read the verified complaint in rem.
3. The matters contained in the within verified complaint in rem are true and accurate to the best of my knowledge, information and belief.
4. The source of my information and the grounds for my belief are information provided by other law enforcement officers, and various official files and records, including those of the Federal Bureau of Investigation, and information provided by law enforcement agents from the Republic of India.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge, information and belief.

Dated: Brooklyn, New York  
December 12, 2024



---

John Reuther  
Task Force Officer  
Federal Bureau of Investigation